Developing EU Cybercrime and Cybersecurity: On legal challenges of EU institutionalisation of cyber law-making

Elaine Fahey

Introduction

The EU has evolved much cyber law over the course of two decades. The EU has approached cyber regulation with a particularly unwieldly mix of powers, sanctions and the development of new actors and agencies. Cyber law-making arguably exposes the EU as a weak global governance actor, conflicted, beholder to private actors and vexed by its competences (Carrapiço and Barrinha, 2018: 1254). EU cyber law-making reveals a partially institutionalised field, with incomplete and awkwardly non-intersecting competences, straddling incomplete Security and Digital Single Market policies, evolving sanctions and new agencies. Cyber laws and policies fall as a law-making exercise only partly within EU security (Fahey, 2020: 1; Christou, 2019: 278). This chapter shows the EU caught between complex global challenges and contested taxonomies. The EU harbours multiple conflicting definitions of cybercrime between actors and entities and multiple working definitions of cybersecurity. Some key terms also lack common definition in the EU context e.g. cyber defence, albeit as a key competence of the EU Member States. The EU lacks sufficiently robust institutions, agencies or actors to implement cyber security and risks conflicts and impingement upon many fundamental rights through its partial institutionalisation of a field. As a result, the EU as a Global cyber actor risks becoming an inadequate international actor. Global law-making efforts, e.g. on a Treaty, is advancing but the EU's engagement therewith will likely prove legally problematic as to the autonomy of EU law.

Methodology

This chapter will use the methodology of EU international relations law and international relations to develop the account. The chapter draws from EU internal market law and ECHR law also to develop its account.

Research question

Does the EU lack sufficiently robust institutions, agencies or actors to implement cyber security through its partial institutionalisation of a field? Is it a weak global actor through its own weak instituitonalisation through its approach to its internal law-making?

The chapter examines: EU cyber law-making: on its subjects and objects; EU cyber actors; EU cybercrime as next generation criminal law; EU cybersecurity; EU external law-making, followed by Conclusions.

EU cyber law-making

EU Cyber law-making:- on subjects and objects

Although not unique to law-making beyond the State, arguably one of the most complex elements of cyber law-making is its mainly composite and multi-level structure. Cyber law-making, from cybercrime to cybersecurity, governance and regulation appears increasingly defined by private actors standards, regimes and roles who assume by both stealth and also by design significant roles in regimes (Carrapiço and Farrand, 2017: 245; Carrapiço and Farrand, 2018: 200). The freedom from regulation and governance has 'iconically' defined cyber regimes from the outset (e.g. the internet), giving private actors the ultimate say (Barlow, 1996).

The problematisation of cybercrime as a regulatory subject has long been disputed. There has long been much confusion about the risks posed by cybercrime and the consensus that it exists (Wall, 2008: 861, 862). Few national level prosecutions, fueled by reports of a high rate of cybercrime activity, render it problematic (Bendiek and Porter, 2013: 166-167). The Commission published its new Eurobarometer report on Internet security and cybercrime in early 2019 showing that Europeans were increasingly concerned about cybercrime, with 79% of them believing that the risk of becoming a victim of cybercrime is greater than in the past (Eurobarometer, 2019). The EU had passed 15 out of 22 legislative proposals on the EU Security Union by 2019 (European Commission, 2019c).

Cyber Actors:

Responsibility for EU Cybercrime and cyber security was historically divided in the first post-Lisbon Commission between the Vice-President of the Commission, Nelie Kroes

(Cyber security/ Digital Agenda) and the then Commissioner for Home Affairs, Cecilia Malmstrom (Cybercrime). The original joint involvement of three Commission DG's: Home Affairs, Justice and Information Society, as well as numerous agencies in the development of an EU cyber strategy is indicative of the challenges of internal security. This has a considerable external or global dimension and the development of an EU cyber strategy is touted also as a major success as regards inter-institutional cooperation. In the new Commission of 2019 cybercrime and security traverse different DG Internal Market; DG Connect (CNECT) (DG CNECT: Communications Networks, Content & Technology was in charge of all directorates - Deputy Director-Khalil Rouhana; Directorate H Digital Society, Trust & Cybersecurity K. Rouhana (acting) H1 Cybersecurity Technology & Capacity Building - M. González-Sancho; H2 Cybersecurity & Digital Privacy Policy - J. Boratynski; Digital Single Market – Directorate F: Digital Single Market – Gerard de Graaf and DG HOME: General Migration and Home Affairs. Directorate D4 – Cybercrime – Cathrin Bauer-Bulst). It is a very broad, institutionalised and balanced composition of teams on one level, but also separates content in ways which are not necessarily aligned with actual law-making.

Considerable differences between the two fields of the digital single market and internal market exist from a legal perspective- as an incomplete sub-field thereof, despite the use of broader internal market legal policies here. Security and internal market matters have a complex intersection in cyber matters and it remains to be seen how much the legal infrastructure will align.

b. The European Union Agency for Cybersecurity (*ENISA)*

ENISA constitutes one of the earliest EU efforts at cyber institution-building. Originally, ENISA had a restricted mandate and liaised predominantly with largely national law enforcement bodies on the security aspects of cybercrime. ENISA was involved in establishing the European cybersecurity certification framework by preparing certification and helping EU Member States which would request it to handle cybersecurity incidents. It is also supported the coordination of the EU in case of large-scale cross borders cyber-attacks and crises (Fahey, 2014: 53). This task built on ENISA's role as secretariat of the National Computer Security Incidents Response Teams (CSIRTs) Network, established by the Directive on security of network and information systems (European Parliament and the Council, 2016a: 17). ENISA was concerned with improving the EU's resilience against cyber-

attacks, notably by capacity-building, but also by exchanging information and providing analyses. Furthermore, at the request of Member States, ENISA can assist Member States in the assessment of incidents having a substantial impact by providing expertise and facilitating the technical handling of such incidents. It also provides support to *ex-post* technical inquiries and created the secretariat for the CSIRTs network.

In 2017, a new Act providing for a Cybersecurity Agency was adopted coming into force in 2019 (European Parliament and the Council, 2019) which would give ENISA more tasks and resources to assist Member States, e.g. through a stronger mandate, a permanent status and more resources. In particular, a core plank of its work would relate to an EU framework for cybersecurity certification as an EU-wide framework, thereby embedding it into systems of law-making.

Whether ENISA can evolve into a major actor remains to be seen in its latest set-up. Its international activities are of note with key partners e.g. capacity building with Japan (Vosse, 2019: 3.12), also deepening cyber security cooperation provided for in the EU-Japan Economic Partnership Agreement, chapter on digital trade (EU-Japan, EPA 2018: Article 8.80). However, its reliance on a vast multitude of sub-(national) and technical actors remains it core challenge- 'bottom up' and 'top down'- a group which continues to evolve.

EU Cybercrime Centre: 'EC3'

Another actor of note is the EU Cybercrime Centre, with the acronym "EC3", which was established in early 2012. It became operational by 2013 as a 'desk' within Europol. The placement of the Cybercrime Centre 'within' Europol was explicitly part of the Action Plan to implement the Stockholm Programme (European Commission, 2010b: 38). Also, the Cybercrime Centre was charged with the implementation of Directives on attacks against Information Systems and the Directive adopted in 2011 on combating the sexual exploitation of children online and child pornography (European Commission 2012b; European Parliament and the Council, 2011). Its purpose was thus institutional and strategic and has been established within an evolving EU agency, the European Police Office, Europol, thereby forming an EU focal point in fighting cybercrime, fusing information and informing Member States of threats. Europol was asserted at the launch of the Cybercrime Centre to lack resources to gather information from a broad range of sources and to lack the specific capacity to deal with requests

from law enforcements agencies, the judiciary and the private sector (European Commission, 2012a: 1-2). The novelty of the Centre was that it purported to adopt a "cross-community approach", to exchange information beyond the law enforcement community. It would develop a common standard for cybercrime reporting and to become the collective voice of cybercrime investigation. The Cybercrime Centre was to post liaison officers to the European Commission and the European External Action Service as well as to EU agencies (Nielsen, 2012).

However, the Centre had no express link to cyber security. Moreover, its express function is to disrupt organized crime networks and monitor illegal activities, which begs the question as to what precisely was illegal under EU law, given the broad parameters of the existing Framework Decisions and the discretion accorded to Member States therein. The establishment of an EU agency to engage in cybercrime monitoring *prior* to the development of a coherent cybercrime and cyber security strategy indicates the evolving nature of the EU internal policies.

The EU as an International Cyber Actor: Centralised EU Action through the prism of International Law

Organisation for Economic Co-operation and Development (OECD)
United Nations General Assembly (UNGA)
Organisation for Security and Co-operation in Europe (OSCE)
International Telecommunication Union (ITU,)
World Summit on the Information Society (WSIS)
Internet Governance Forum (IGF)

Table of international organisations where the EU engages in cyber law-making

Although cyberspace has had a difficult relationship with international law and the Nation State, the EU has a 'healthy' presence in a variety of international fora (e.g. Odermatt, 2018: 354). The Cybersecurity Strategy of the European Union (European Commission, 2013b: 3) outlines the goal of establishing a coherent international cyberspace policy in order to be able to promote EU values). Thus, significant cooperation is also ongoing between the EU and the Council of Europe in the area of developing best practice in international

governance, discussed below. The EU has also been involved in bilateral actions with many partners as to cyber activities e.g. EU-US and South Korea. The EU is also active in many forums where cyber matters are being developed e.g. Organisation for Economic Co-operation and Development (OECD), the United Nations General Assembly (UNGA), the Organisation for Security and Co-operation in Europe (OSCE), International Telecommunication Union (ITU,) the World Summit on the Information Society (WSIS) and the Internet Governance Forum (IGF). Cyber defence policy also requires cooperation with key partners such as NATO, given that cyber defence is a core task of NATO. One of the key challenges of EU international action is the presentation of coherent positions where within its own organisational policies, rules and practices, a multiplicity of positions exist.

The Conclusions on Cyber Diplomacy adopted by the Council on 11 February 2015 gave a mandate to the EU and its Member States to uphold freedom, security and prosperity in the cyberspace: this includes *inter alia*, promotion and protection of human rights, application of international law and norms of responsible state behaviour, internet governance, fight against cybercrime, protection of networks and systems of government and critical infrastructure, international cooperation, capacity building, competitiveness in the digital market, strategic engagement with key partners. Cyber diplomacy toolbox measures were developed, including restrictive measures, to be used to prevent and respond to malicious cyber activities (Council, 2015).

In 2018, the European Council, in its Conclusions, called on institutions and Member States to implement the measures referred to in the Joint Communication on increasing resilience and bolstering capabilities to address hybrid threats, including the work on the tracing of cyber-attacks and the practical use of the cyber diplomacy toolbox (European Council, 2018a: 6). As a follow up, the Council adopted the necessary legal acts establishing a framework for targeted restrictive measures to deter and respond to cyber-attacks with a significant effect which constitute an external threat to the Union or its Member States (Council of the European Union, 2019). These acts allow for restrictive measures to be applied in response to cyber-attacks with a significant effect against third States or international organisations, pursuant to Article 21 TEU and they significantly enhance the unitary nature of the EU's response. They looked set to be deployed in Summer 2020.

EU Cybercrime as next Generation EU Criminal Law

Overview

EU Cybercrime law is scattered amongst legal instruments. EU Cybercrime policy begun with the Framework Decision on attacks against information systems in 2005 (Council of the European Union, 2005). The Framework Decision provided for the criminalisation of online and offline conduct, provided for serious penalties and jurisdictional rules. While some argue that soft law has been gradually replaced by hard law or actual legislation in the form of a Directive in cybercrime, a rising number of instances are also evident where private actors set standards and where they enforce them as judge and jury of conduct (Carrapico & Farrand, 2018: 245). It is a trend increasingly evident not just in cybercrime law but broadly in the external JHA matters, which also represents a worrisome state of EU governance and accountability standards (Christou, 2018: 355).

The legal basis for EU Cybercrime action: top-down 'strength"?

Internal EU cybercrime policy has historically been situated in an *internal market* rationale (Fahey, 2014: 50; Fahey, 2020: 8). Internal EU cybercrime and security policies additionally have a relevance to the functioning of the internal market, to the safety of consumers and business. However, cybersecurity most recently takes its legal origins in CFSP measures. This bifurcated understanding of regulatory structures between the internal market and the CFSP stands as an important reminder of the highly confused, incomplete traversing of ideas, institutions and actors afflicting cyber matters.

Post-Lisbon, there are ostensibly several legal bases in the treaties *outside* of the internal market rationale to legislate in order to regulate cybercrime and security. For example, there are grounds in the treaties to legislate for procedural EU Criminal law in Article 82 TFEU, allowing for the European Parliament and Council to establish minimum rules to the extent necessary to facilitate mutual recognition of judgments and judicial decisions and police and judicial cooperation in criminal matters having a cross-border dimension. In Article 83 TFEU, the EU can enact substantive criminal law. More specifically, Article 83(1) TFEU provides that Parliament and Council may establish minimum rules concerning the definition of criminal law offences and sanctions in the area of particularly serious crime which have a cross border dimension resulting from the impact of such offences or need to combat such offences jointly. This provision includes thereafter a list of crimes in which the EU has legislative competence

which specifically includes terrorism. Article 83(2) TFEU also provides for harmonisation to ensure the effective implementation of EU policy already subject to harmonisation measures. Post-Lisbon, a legal basis for cybercrime and cybersecurity seems easily grounded on these legal bases with respect to serious crime across borders. Put differently, terrorism does not appear as the only rationale of EU cyber policies and the emphasis on the impact of non-regulation of cybercrime on the internal market is notable. The gap in the type of legal instruments appears thus as significant.

Directive

A Directive adopted in late 2013 'Cybercrime Directive' places emphasis in particular upon a Strategy to fight *new* methods of cybercrime, for example, large scale 'botnets' i.e. networks of computers with a cross-border dimension (European Parliament and the Council, 2013). The Commission has invoked Eurobarometer surveys on cybercrime referencing the legal uncertainty surrounding the protections for consumers engaging in online payments (European Commission, 2012). However, in this regard, in contrast to the Framework Decision, it is not necessarily a superior regulatory instrument. As a Directive, disparities inherent in its implementation practices may cause its provisions to be unevenly interpreted across the Member States, which seems undesirable if the desire is to regulate holistically.

EU cybersecurity: in search of a definition?

Overview

The historical absence of a common EU framework on cyber security has been the subject of much critique, from inside and outside the EU institutions, similar to the absence of cyber-security strategies at national level. The EU law-making in cybercrime and cybersecurity started in policy terms most concretely with a Cybersecurity Strategy in 2013, which defines cybersecurity broadly. Cybersecurity is there referred to as "safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure" (EU Cybersecurity Strategy, 2013: 3). What is significant about the Strategy is the dominance of security therein and the lack of specificity about the definition of cybercrime to be deployed. Others point to the narrower definition of cybersecurity used by the EU Agency for Network and Information Security (ENISA), distinguishing cybercrime, cyber espionage and cyber warfare (Odermatt, 2018: 354). Despite being explicitly labelled a 'Cybersecurity

Strategy,' the EU's Strategy has a complex engagement with cybercrime therein relegated to[…] "a broad range of different criminal activities where computers and information systems are involved either as a primary tool or as a primary target" (European Commission, 2013: 3).

An overwhelming number of legal and policy documents relating to cybersecurity often begin with a conceptual discussion about what exactly cybersecurity means (Odermatt, 2018: 356). It is a term which is often ambiguous and ill-defined partly because of the evolving nature of the threats. There is no explicit basis for it in EU law, largely because the EU has traditionally related to the economic effects of cyber-attacks in order to legislate in cybercrime (Odermatt, 2018: 360). The EU's Strategy for cyber security was finally published in early 2013 and it follows many less than successful policy initiatives. These include a proposal for an Networks and Information Policy in 2001, soft law strategies and various programmes, instruments and policies on so-called Critical Infrastructure, policies that did not establish binding legal obligations upon the operators of critical infrastructures (Fahey 2014: 49). This reliance upon soft law to regulate cyber risk has been overtaken by more recent legislative matters. Cyber security is depicted in the EU's Strategy as referring to 'the safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure' (European Commission, 2013: 3). Cyber security features prominently in the EU Security Union Strategy in 2020 (European Commission, 2020: 7-10). There, cybersecurity by design, including certification schemes under the Cybersecurity Act and deepening cooperation between ENISA and the European Data Protection Board, are asserted. A further Joint Cyber Unit to build trust between actors in the cybersecurity system and the Member States is envisaged (European Commission, 2020: 9).

This generates three definitional questions concerning cyber risk. Firstly, the relationship of Cyber Security and confidentiality of information with data protection matters is ostensibly of much significance from the type of harm formulation, but is only beginning to emerge. Secondly, this definition presupposes the relevance of militarisation to it conceptually. While the text of the Council of Europe Convention itself does not mention terrorism, a listed activity on the website of the Council of Europe is cyber-terrorism (Council of Europe, 2020). Thirdly, the Strategy describes *cybercrime* to include a range of different criminal activities, not precisely as in the Convention (European Commission, 2013: 3). Its definition of cybercrime has thus generated many key legal definitional questions.

The Cybersecurity 'Act', 2019

Some key EU Criminal law Directives deploy maximum harmonization on the bases of Article 82(2) and 83(1) TFEU in order to regulate the sexual exploitation of children online and child pornography as measures for judicial cooperation in criminal matters of the EU (e.g. European Parliament and the Council, 2011). On the one hand, examples such as these show the extraordinarily broad parameters of cyber matters. On the other hand, there are even more striking developments. For example, on 13 September 2017 the Commission adopted a cybersecurity package based upon a Regulation formulated as a so-called 'Cybersecurity Act,' on the basis of Article 114 TFEU in the context of the Digital Single Market Strategy (European Parliament and the Council, 2019). the Act is intended to set up a high level of cybersecurity, cyber resilience and trust within the Union with the objective of ensuring the proper functioning of the internal market. The changes this new EU Regulation sought to bring about relate to both: a comprehensive reform of ENISA and the creation of a certification framework. It brings into sharp focus earlier efforts at development of EC3 as a mere desk in Europol, as discussed above. The Agency established will thus 'succeed' ENISA as established by Regulation No. 526/2013 as a significant step in the 'agencification' of cyber policies - and its consequent deeper institutionalisation (Fahey, 2018: 1-27). The Act thus represents a definitive step towards an empowered framework through internal market competences. Yet other criminal law competences are not used and the enforcement of the internal market may be said here to be 'light'.

However, cybersecurity, as introduced above, new CFSP cyber sanctions are also a core plank of cybersecurity and are discussed next.

EU Cyber sanctions

The EU has adopted sanctions against 35 countries and four thematic sanctions regimes regarding chemical weapons and terrorism and most recently cyber sanctions and human rights (Portela 2019: 1-3; Eckes, 2019: 206). The EU is the world's second-most active user of restrictive measures after the United States (US). On 18 October 2018, the European Council adopted conclusions calling for work on the capacity to respond to and deter cyber-attacks through EU restrictive measures. On 17 May 2019, the Council establishing a framework for targeted restrictive measures to deter and respond to cyber-attacks with a significant effect

which constitute an external threat to the Union or its Member States. These acts also allow for restrictive measures to be applied in response to cyber-attacks with a significant effect against third States or international organisations, pursuant to Article 21 TEU. It is a striking executive-led legal formula to deploy. Yet it occurs in a field where the Court of Justice has become gradually more pervasive and extended its own powers of review in the area of the CFSP.

This leads to a broader discussion of actors and cyber law-making.

EU External Law-Making

Cyberspace has had a difficult relationship with international law and national law because there is still no uniform cyber law as an instrument of international law which is all encompassing. Cyber law-making is ostensibly a global affair and yet its de-centralisation through according powers to powerful global private entities continues to be a paradoxical reality (Carrapiço and Farrand, 2018: 245). The role of such private entities in cyber law-making appears as the antithesis of global law-making. However, there is no global cyber agreement and Russia, the US and China remain key stumbling blocks to global reform rather than partners for a united cyber world.

UN level

The UN created an expert group to draft a new cyber Treaty to begin work in 2020, on the basis of a Russian text draft (Lederer, 2019). It is understood by Russia to be an alternative to the Council of Europe Cybercrime Convention (discussed below), whereas others such as the EU see the Treaty less about cybercrime and more about internet control (Sherman and Raymond, 2019). More generally, the international community has moved one step closer to the risk of fragmentation in recent years, with blocs split between China, Russia and the West. Having various processes discussing the application of international law to cyberspace, initiated by two different groups of States with divergent approaches on the application of some norms of international law, contributes to the risk of geographical fragmentation (Delerue, 2019: 1-4). It is thus a more fragile context broadly overall for Europe to engage with and a complex background tapestry. Whether this latest Treaty can successfully evolve remains to be seen.

Council of Europe

The Council of Europe Cybercrime Convention ('Budapest Convention') forms a 'transnational gold standard' for cybercrime regulation. The Budapest Convention on Cybercrime was opened for signature in 2001. Membership in this treaty increases continuously and any country able to implement its provisions may seek accession. By July 2020, 65 States had become Parties and a further 8 had signed it or been invited to accede.[1] The Budapest Convention is supplemented by an additional Protocol on Xenophobia and Racism committed via computer systems. Much EU Criminal law has its origins in Council of Europe Conventions, because of their tendency to set best international practice and to organise regimes of considerable merit. The Cybercrime Convention is now seen as major transnational venue for internet reform, but this has not always been the case. The Cybercrime Convention has been criticised by civil society as too heavily reflecting law enforcement standards and its relationship with the broader regulatory framework of the Council of Europe and large-scale standards on data protection remains less than persuasive (Brown, 2014: 3). In particular, the Convention is perceived by privacy advocates as a broad, but not the broadest international forum, whereby the UN forms the apex thereof (Brown, 2014: 37). The US is not a member of the Council of Europe but took a significant part in the drafting of the Council of Europe Cybercrime Convention and has signed and ratified it domestically, as have approximately half the Member States of the EU (Fahey, 2014: 368). In the wake of the US National Security Agency (NSA) affair, the Cybercrime Convention was touted by the US in EU-US negotiations on its aftermath recently as setting particularly high international standards in privacy and data protection and as evidence of the willingness of the US to lead and set such standards (Fahey, 2014: 55-57).

The Council of Europe Cybercrime Convention adopts a broad perspective on cybercrime. In fact, can be criticised for its overbroad content, its lack of provision for cross-border enforcement and its obligations imposed upon Internet Service Providers and also that it does not purport to regulate cyber security. The Convention distinguishes between four types

[1] 65 countries are party to the Budapest Convention: for the latest list see: https://www.coe.int/en/web/cybercrime/parties-observers, accessed 8.09.2020.

of offences which as a typology may be argued not to be wholly consistent in that three of the types of offences focus upon legal protection whereas the fourth does not and leads as a result to overlap between the categories. In addition, criminal acts such as cyber terrorism or phishing cover acts may fall within several categories. The Convention does not contain as many definitional conceptions of cybercrime as other regional legislative models do, which may appear surprising given its tendency towards harmonisation rather than closing gaps in regulation. Nonetheless, it is the most far-reaching multilateral agreement on cybercrime in existence, purporting to harmonise national legislation procedurally.

There is a particular emphasis in contemporary Council of Europe Cybercrime policy as to its reform of inter alia relevance of jurisdiction, Yet what should the Convention be aiming for? Is its focus in reality conventional rather than progressive? Such a focus appears troubling from the transnational 'gold-standard', as one centered exclusively around enforcement as opposed to rights-based rule-making. Its unequivocal stance as the leading cyber law instrument draws attention to its less than holistic integration of other regimes even within the Council of Europe, its rights-based conceptions of rule-making in this field and its incompleteness as an instrument. The lack of any meaningful engagement between the Convention and the reform of related UN measures also raises the question as to regime interaction or lack thereof and the ideal of global set of laws.

The Parties to the Budapest Convention have been searching for solutions for some time, that is, from 2012 to 2014 through a working group on transborder access to data and from 2015 to 2017 through the Cloud Evidence Group. In 2017, negotiations commenced in on: efficient mutual legal assistance; direct cooperation with providers in other jurisdictions; a Framework and safeguards for existing practices of extending searches transborder and Rule of law and data protection safeguards (Council of Europe, 2017). The Parties to the Convention have been looking to reform access to electronic evidence by judicial and police authorities through a Second Additional Protocol which would address those challenges by ensuring greater international cooperation. The negotiations on the Protocol are ongoing but could prove to be significant also at broader UN level.

The limitations of the EU as an international organization (IO)

These international negotiations are significant because the EU role there is complex. The EU has had to consider the protection of privacy and personal data (as specified in

the General Data Protection Regulation (GDPR) (European Parliament and the Council, 2016b), the e-Privacy Directive (European Parliament and the Council, 2002) and the Data Protection Directive for Police and Criminal Justice Authorities) (European Parliament and the Council, 2016c) and the development of EU rules on electronic evidence relative to third countries. The EU has issues as to consistency with respect to e-evidence regimes and third countries, in particular the US. Two recommendations to participate in the Second Additional protocol and to open negotiation with the US were being adopted by the Commission at the same time and the Commission and other EU institutions are observers in the Protocol Drafting Plenary (European Commission, 2019). An EU specific 'disconnection' clause raises challenges for a guarantee that only EU law, whether existing or future, will be applied as between EU Member States. However, the Budapest Convention is said already to contain a provision which should meet the concerns of the European Union not to compromise its normative acquis or the autonomy of its legal order (Council of Europe, 2019: 34-36). Whether this will prove acceptable to the CJEU is another matter. It highlights the manifold challenges faced by the EU.

Conclusions

The EU's cyber law-making has for some time dominated by weak efforts at institutionalisation and few actors. This will radically change given the unfolding internal market directions of cyber law-making. The reality of contemporary cyber law is, however, dominated by a need to use a clumsy mix of CFSP, criminal law powers and sanctions for its effectiveness. The overall matrix of law-making appears increasingly skewed in different directions, destined towards partial institutionalisation and weaker actors. EU law often appears divided between cybercrime and cybercrime in a manner which is not always logical or effective. However, like many areas of EU law it may rapidly evolve through institutionalisation, albeit that its structure, architecture and foundations remain open to contestation. Ultimately many significant global develops taking place provide for significant input, participation and development of cyber law-making. Whether the EU is able to so do remains to be seen.

Credits: This chapter draws from Fahey, E. (2020). Institutionalising EU Cyber Law: Can the EU institutionalise its many subjects and objects? Vienna: Vienna Institute for European Integration Research (EIF) Working Paper Series 2/2020. Thanks to Ivanka Karaivanova for research assistance.

Bibliography:

Barlow, J. (1996) 'Declaration of Independence of Cyberspace', Electronic Frontier Foundation, 08.02.1996. Available from: https://www.eff.org/cyberspace-independence Last accessed 08 September 2020.

Bendiek, A., Porter, A. (2013) 'European Cyber Security Policy within a Global Multistakeholder Structure', *European Foreign Affairs Review,* Volume 18 Issue 2, 155-180.

Bernik, I.(2014) *Cybercrime and Cyber Warfare*, London and Hoboken: John Wiley and Sons.

Brown, I. (2014) 'The feasibility of transatlantic privacy protective standards for surveillance', *International Journal of Law and Information Technology*, Volume 23 Issue 1, 23-40.

Buchan, R. (2018) *Cyber-Espionage and International Law*, Oxford and London: Hart Publishing.

Carrapico, H. and Barrinha, A. (2017) The EU as a Coherent (Cyber)Security Actor?. *Journal of Common Market Studies*, Volume 55, 1254– 1272.

Carrapico, H. and Farrand, B. (2017) 'Dialogue, partnership and empowerment for network and information security': the changing role of the private sector from objects of regulation to regulation shapers. *Crime, Law and Social Change*, Volume 67, Issue 3, 245-263.

Carrapiço, H. and Farrand, B. (2018) 'Blurring Public and Private: Cybersecurity in the Age of Regulatory Capitalism'. In: Bures, O. and Carrapiço, H. (eds) *Security*

Privatization : How Non-Security-Related Businesses Shape Security Governance, Cham : Springer International Publishing AG, 197-218.

Christou, G. (2018) 'The Challenges of Cybercrime Governance in the European Union', *European Politics and Society*, Volume 19, Issue 3, 355-375.

Christou, G. (2019) The collective securitisation of cyberspace in the European Union, *West European Politics*, Volume 42, Issue 2, 278-301.

Council of Europe (2001) 'Convention on Cybercrime', European Treaty Series, No.185 (Budapest), 23.11.2001, Available from: https://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf. Last accessed 15 September 2020, 25 pages.

Council of Europe (2017) 'Terms of Reference for the preparation of a draft 2nd Additional Protocol to the Budapest Convention on Cybercrime' T-CY'(2017)3, 5 pages.

Council of Europe (2019) 'Legal Opinion on Budapest Cybercrime Convention: use of disconnection clause in Second Additional Protocol to the Council of Europe Convention on Cybercrime', 29.04.2019, Available from: https://www.coe.int/en/web/dlapil/-/use-of-a-disconnection-clause-in-the-second-additional-protocol-to-the-budapest-convention-on-cybercri-1. Last accessed 08 September 2020.

Council of the European Union (2005) 'Council Framework Decision 2005/22/JHA of 24 February 2005 on Attacks Against Information Systems', Official Journal L 69, 16.03.2005, 69/67, 5 pages.

Council of the European Union (2014) 'EU Cyber Defence Policy Framework', - 15585/14 (Brussels), 18.11.2014. 14 pages.

Council of the European Union (2015) 'Council Conclusions on Cyber Diplomacy,' 6122/15 (Brussels), 11.2.2015

Council of the European Union (2019) ‘Legislative Acts and other Instruments - Decision Concerning Restrictive Measures Against Cyber-Attacks Threatening the Union or its Member States’, 7299/19 (Brussels), 14.05.2019, 19 pages.

Delarue, F. (2020) *Cyber Operations and International Law*, Cambridge: Cambridge University Press.

Drewer, D. and Ellermann, J. (2012) ‘Europol’s data protection framework as an asset in the fight against cybercrime’, Europol, 19.11.2012. Available from: https://www.europol.europa.eu/publications-documents/europols-data-protection-framework-asset-in-fight-against-cybercrime, Last accessed 08 September 2020.

Eckes, C. (2019) ‘The Law and Practice of EU Sanctions’. In: Blockmans, S. and Koutrakos, P. (eds.) *Research Handbook on EU Common Foreign and Security Policy*, Cheltenham and Northampton: Edward Elgar, 206-229.

Eichensher, K. (2015) ‘The Cyber Law of Nations’, *Georgetown Law Journal*, Vol.103, 317-380.

Ekengren, M. and Simon H., (2019) ‘Explaining the European Union's Security Role in Practice’, *Journal of Common Market Studies*, pp.1-19.

Eurobarometer (2019) ‘Europeans’ Attitudes Towards Internet Security’, March 2019. Available from: https://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/survey/getsurveydetail/instruments/special/surveyky/2207. Last accessed 08 September 2020.

European Commission (2001) ‘Communication From The Commission To The Council, The European Parliament, The European Economic And Social Committee And The Committee Of The Regions - Network and Information Security: Proposal for a European Policy Approach’, COM(2001) 298 final, (Brussels), 27 pages.

European Commission (2006) ‘Communication From The Commission To The Council, The European Parliament, The European Economic And Social Committee And The Committee Of The Regions - Strategy for a Secure Information Society: “Dialogue, Partnership and Empowerment’, COM(2006) 251 final, (Brussels), 10 pages.

European Commission (2007) ‘Communication From The Commission To The European Parliament, The Council And The Committee Of The Regions - Towards a General Policy on the Fight Against Cyber Crime’, COM (2007) 267 final, (Brussels), 10 pages.

European Commission (2009) ‘Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions - on Critical Information Infrastructure Protection: Protecting Europe from large-scale cyber-attacks and disruptions: enhancing preparedness, security and resilience’, COM (2009) 14 final, (Brussels), 11 pages.

European Commission (2010a) ‘Proposal for a Directive of the European Parliament and Council on attacks against information systems and repealing Council Framework Decision 2005/222/JHA’, COM(2010) 517 final, (Brussels), 18 pages.

European Commission (2010b) ‘Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions - Action Plan Implementing the Stockholm programme’, COM(2019) 171 final, (Brussels), 68 pages.

European Commission (2010c) ‘Communication from the Commission to the European Parliament and Council - The EU Internal Security Strategy in Action: Five steps towards a more secure Europe’, COM(2019) 673 final (Brussels), 24 pages.

European Commission (2011) ‘Communication from the Commission to the European Parliament and Council - First Annual Report on the implementation of the EU Internal Security Strategy’, COM(2011) 790 final (Brussels), 19 pages.

European Commission (2012a) ‘Press Release - Cybercrime: EU citizens concerned by security of personal information and online payments’, (Brussels), 9.07.2012, IP/12/751.

European Commission (2012b) ‘Press Release - EU Cybercrime Centre to Fight Online Criminals and Protect E-consumers’, (Brussels), 28.03.2012, IP/12/317, 4 pages.

European Commission (2013a) ‘Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace’ JOIN 1 Final (Brussels), 20 pages.

European Commission (2013b) ‘Commission Staff Working Document - Proposal for a Directive of the European Parliament and of the Council Concerning measures to ensure a high level of network and information security across the Union’ SWD 32 Final (Strasbourg), 160 pages.

European Commission (2019a) ‘Recommendation for a Council Decision Authorising the Opening of Negotiations in View of an Agreement between the European Union and the United States of America on Cross-Border Access to Electronic Evidence for Judicial Cooperation in Criminal Matters’, COM 70 final, (Brussels) 5.2.2019, 13 pages.

European Commission (2019b) ‘Recommendation for a Council Decision Authorising the Participation in Negotiations on a Second Additional Protocol to the Council of Europe Convention on Cybercrime (CETS No. 185), COM(2019) 71 final, (Brussels), 5.2.2019, 11 pages.

European Commission (2019c) ‘Press Release - A Europe that Protects: 15 out of 22 Security Union Legislative Initiatives Agreed So Far’, (Brussels), 20.03.2019, IP/19/1713.

European Commission (2020) ‘Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on the EU Security Union Strategy’,

COM(2020) 605 final, (Brussels), 24.07.2020, 28 pages.

European Council, (2018a) ‘From General Secretariat of the Council to Delegations - Conclusions 28 June 2018’, EUCO 9/18, (Brussels), 11 pages.

European Council (2018b) ‘From General Secretariat of the Council to Delegations - Conclusions 18 October 2018’, EUCO 13/18, (Brussels), 5 pages.

European Parliament and the Council (2002) ‘Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)’, Official Journal L 201/37, 31.07.2002.

European Parliament and the Council (2011) ‘Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on Combating the Sexual Abuse and Sexual Exploitation of children and Child Pornography, and replacing Council Framework Decision 2004/68/JHA’, Official Journal L 335/1, 17.12.2011.

European Parliament and the Council (2013) ‘Directive 2013/40/EU On Attacks Against Information Systems and Replacing Council Framework Decision 2005/222/JHA’, Official Journal L 218/8, 14.08.2013.

European Parliament and the Council (2016a) ‘Directive 2016/1148 - Concerning Measures for a High Common Level of Security of Network and Information Systems across the Union’ Official Journal L 194/1, 06.07.2016.

European Parliament and the Council (2016b) ‘Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)’ Official Journal L 119/1, 04.05.2016.

European Parliament and the Council (2016c) ‘Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons

with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA' Official Journal L 119/89, 04.05.2016.

European Parliament and the Council (2019) 'Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and On Information and Communications Technology Cybersecurity Certification and Repealing Regulation (EU) No 526/2013 (Cybersecurity Act), Official Journal L 151/15, 07.06.2019.

Fahey, E. (2014) 'The EU's Cybercrime and Cybersecurity Rule-Making: Mapping the Internal and External Dimensions of EU Security', *European Journal of Risk Regulation*, Volume 5 Issue 1, 46-60.

Fahey, E. (2018) (ed,) *Institutionalisation beyond the Nation State*, Heidelberg: Springer Publishing.

Fahey, E. (2020). Institutionalising EU Cyber Law: Can the EU institutionalise its many subjects and objects? Vienna: Vienna Institute for European Integration Research (EIF) Working Paper Series 2/2020.

Fahey, E., Odermatt, J. and O'Loughlin, E. (2019) 'Whose Global law?: Comparative, Regional and Cyber Approaches to Law-Making*',* City Law School (CLS) Research Chapter: No. 2019/02.

Fishera, M. (2013) 'Criminal Law beyond the State: The European Model', *European Law Journal,* Volume 19, Issue 2, 174-200.

Gercke, M. (2012) 'International Telecommunication Union: Understanding Cybercrime: Phenomena, Challenges and Legal Reponses'. Available from: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf, September 2012. Last accessed 08 September 2020.

Goldsmith, J. (2001) 'The Internet and the Legitimacy of Remote Cross-Border Searches', *University of Chicago Legal Forum,* Volume 2001 Issue 1, 103-118.

Hathaway, O., Crotoff, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W. and Spiegel, J. (2012) 'The Law of Cyber-Attack', *California Law Review,* Volume 100 (no issue) 817-886.

Lederer, E. (2019) 'UN gives green light to draft treaty to combat cybercrime' AP News. https://apnews.com/79c7986478e5f455f2b281b5c9ed2d15 . Last accessed 08 September 2020.

Nielsen, N. (2012) 'EU cybercrime chief fears massive proliferation' 18.09.2012. Available from: https://euobserver.com/justice/117569. Last accessed 08 September 2020.

Odermatt, J. (2018) 'The European Union as a Cybersecurity Actor'. In: Blockmans, S. and Koutrakos, P. (eds.) *Research Handbook on EU Common Foreign and Security Policy*, Cheltenham and Northampton: Edward Elgar Publishing, 354-373.

Porcedda, M. G. (2011) 'Transatlantic Approaches to cyber-security and cybercrime'. In: Pawlak, P. (ed.), '*The EU-US Security and Justice Agenda in Action'* (30 December 2011) EU Institute for Security Studies Chaillot Chapter, No 127, Paris: EU Institute for Security Studies, 41-53.

Portela, C. (2019) 'The Spread of Horizontal Sanctions', 07.03.2019. Available from: https://www.ceps.eu/the-spread-of-horizontal-sanctions/. Last accessed 08 September 2020.

Sassen, S. (2017) 'Embedded Borderings: Making New Geographies of Centrality', *Territory, Politics, Governance*, Volume 6 Issue 1, 5-15.

Schmitt, N. M. (ed) (2013) *Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence: Talinn Manual on the International Law applicable to Cyber-Warfare*, Cambridge: Cambridge University Press.

Sherman, J. and Raymond, M. (2019) The U.N. passed a Russia-backed cybercrime resolution. That's not good news for Internet freedom. Washington Post

https://www.washingtonpost.com/politics/2019/12/04/un-passed-russia-backed-cybercrime-resolution-thats-not-good-news-internet-freedom / Last accessed 08 September 2020.

Trauner, F. and Rippoll-Servant, A. (2016) The Communitarization of the Area of Freedom, Security and Justice: Why Institutional Change Does not Translate into Policy Change, *Journal of Common Market Studies*, Volume 54 Issue 6, 1417-1432.

Tsagourias, N. (2019) 'Electoral Cyber Interference Self Determination and the Principle of Non-Intervention in Cyberspace' Blog of the European Journal of International Law, 26.08.2019 . Available from: https://www.ejiltalk.org/electoral-cyber-interference-self-determination-and-the-principle-of-non-intervention-in-cyberspace/. Last accessed 08 September 2020.

Vosse, W. (2019) 'Japan's Cyber Diplomacy', EU Cyber Direct, https://eucyberdirect.eu/content_knowledge_hu/japans-cyber-diplomacy/. Last accessed 08 September 2020.

Wall, D. (2007) *Cybercrime: The Transformation of Crime in the Information Age*, Cambridge and Malden: Polity Press.

Wall, D. (2008) 'Cybercrime and the Culture of Fear: Social Science fiction(s) and the production of knowledge about cybercrime', *Information, Communications and Society*, Volume11 Issue 6, 861-884.